REMARKS

Please reconsider the application in view of the above amendments and the following remarks. Applicants thank the Examiner for carefully considering this application.

Disposition of Claims

Claims 1-3, 8, 11-15, 17-19, 22 and 23 have been cancelled without prejudice or disclaimer. New claims 37-49 have been added and are pending in this application. Claims 37, 41, and 45 are independent. The remaining claims depend, directly or indirectly, from claims 37, 41, and 45.

Claim Amendments

Claims 37-49 have been added and are pending in this application. Applicants respectfully assert that no new matter has been introduced by way of these amendments, as support for these amendments may be found, for example, in Figures 4, 6 and 7 and pages 6, 8, 9, 11, 12, and 14-19 of the originally filed application, and in the originally filed claims.

Rejection(s) under 35 U.S.C § 103

Claims 1-3, 8, 11-15, 17-19, 22, and 23 stand rejected under 35 U.S.C. § 103 as obvious over U.S. Publication No. 2004/0003251 ("Narin") in view of U.S. Publication No. 2001/0027440 ("Tanaka"). Claims 1-3, 8, 11-15, 17-19, 22 and 23 have been cancelled in this reply. Thus, this rejection is now moot. Accordingly, withdrawal of this rejection is respectfully requested.

New Claims

The pending claims are directed to a method and system for implementing trust relationships among entities on a network. By establishing these trust relationships, a client need only login once so long as the authenticating entity trusts entities subsequently accessed by the client. *See, e.g., page 7 lines 10-11 of the application*. For example, a client authenticated by a first server is allowed to obtain access to the resource of a second server, provided that the second server is a trusted partner of the first server. *See, e.g., page 6 lines 9-19 of the application*. More specifically, as recited in the pending claims, the authentication and subsequent providing of access to a resource for a client includes the following course of events:

(i) a client sends an authentication request, including the client's login information, to an authenticating server (*see, e.g., page 15 lines 3-7 of the application*);

(ii) the authenticating server responds to the authentication request by validating the login information and sending the client a response, including an authentication assertion reference (*see, e.g., page 15 lines 8-9 of the application*);

(iii) having been authenticated and now desiring to access a particular resource on the network, the client sends to the server presiding over that resource ('the resource server' for the purposes of this example) an access request that includes the authentication assertion reference (*see, e.g., page 15 lines 9-11 of the application*);

(iv) the resource server, having received the access request from the client, determines the identity of the authenticating server from the authentication assertion reference (*see, e.g., page 15 lines 12-13 of the application*);

(v) the resource server sends to the authenticating server an authentication request, which includes a certificate identifying the resource server (*see, e.g., page 15 lines 15-16 of the application*);

(vi) the authenticating server, having received this authentication request and certificate from the resource server, determines whether the resource server is a trusted partner present in its trusted partner list (*see, e.g., page 15 lines 16-19 of the application*);

(vii) the authenticating server sends the resource server an authentication assertion, when the authenticating server trusts the resource server (*see, e.g., page 15 line 20 of the application*); and

(viii) having received the authentication assertion, the resource server grants the client access to the resource only when the resource server has been deemed a trusted partner by the authenticating server (*see, e.g., page 16 lines 1-3 of the application*).

In accordance with the disclosed subject matter, and as written from the perspective of the client, new independent claim 37 explicitly requires, at least: (i) a client to send an authentication request to a first server; (ii) the first server to issue the client an authentication assertion reference; (iii) the client send to a second server a request to access a resource connected to the second server, where the request provides the second server with the client's authentication assertion reference; (iv) the second server to send the first server an authentication request, where the request provides the first server with a certificate identifying the second server; (v) the first server to determine whether a certificate identifying the second server is present in the first server's trusted partner list; (vi) the first server to send the second server an authentication assertion based on whether the second server's certificate is present in the first server's trusted partner list; (vii) the second server to grant the client access to the request resource based on the authentication assertion. New independent claims 41 and 45 have similar limitations and are written from the respective perspectives of the (resource-granting) 'second server' and the system as a whole, respectively.

In consideration of the cited prior art, Applicants submit that neither Narin, nor Tanaka, nor a combination of both references teach the subject matter disclosed by the pending claims. In particular, neither teaches or suggests a resource server, having received an access request from a client, communicating with the client-authenticating server without first communicating through the client.

Specifically, Narin teaches a rights disbursement model where a content server receives from a client a license request comprising of an identity certificate [0017], such that the identity certificate allows the content server to determine whether it was issued by a trusted identity server. Per Narin, if the issuing identity server is found to be a trusted entity and not present on any exclusion lists [0018, 0019] then the license request is processed [0120]. It is emphasized that, a content server under Narin, having received the request, is not disclosed to communicate with an identity server that issued the certificate accompanying the request [0117-0120]. In contrast, the pending claims require communication between the client-authenticating server and the client-granting server in granting the client access to the resource.

Further, Tanaka teaches a buyer-side credit authentication service suitable for e-commerce purposes [0009]. Per Tanaka, an electronic commerce server and a credit organization server operate in tandem on the buyer-side of an online commercial transaction to provide the seller-side merchant a purchase order that has already been verified with regards to the buyer's credit [0009-0012].

The pending claims are distinguishable from Tanaka for at least the following reasons: (i) Tanaka only requires its client to send a request to one server (the buyer-side electronic server) whereas the claims require the client to request authentication from a first server and request resource access from a second server; (ii) while Tanaka does teach authenticating a client in terms of their credit and granting access to a resource in terms of their purchase, the granting of the resource does not involve a communicative exchange initiated by the resource-granting entity (seller-side merchant) with the client-authenticating entity (buyer-side servers) prior to the granting of client access to the resource.

Finally, Applicants submit that a combination of the Narin and Tanaka references does not render obviousness the subject matter disclosed by the pending claims. Even if one skilled in the art were to combine Narin's teachings of identity and content servers into a unified configuration, as the Examiner suggests Tanaka teaches (*see, e.g., page 3 of Final Office Action citing Tanaka [0162]*), the proposed combination would not disclose at least the aspect of the claimed subject matter pertaining to the communicative exchange initiated by a resource-granting server with a client-authenticating server prior to granting of client access to the resource.

In view of the above, independent claims 37, 41, and 45 are patentable over Narin in view of Tanaka. Dependent claims are patentable for at least the same reasons. In view of that, favorable action in the form of a Notice of Allowability is respectfully requested for new claims 37-49.

Conclusion

Applicants believe this reply is fully responsive to all outstanding issues and places this application in condition for allowance. If this belief is incorrect, or other issues arise, the Examiner is encouraged to contact the undersigned or his associates at the telephone number listed below. Please apply any charges not covered, or any credits, to Deposit Account 50-0591 (Reference Number 03226/503001).

Dated: September 4, 2008

Respectfully submitted,

By /Robert P. Lord/
Robert P. Lord
Registration No.: 46,479
OSHA • LIANG LLP
1221 McKinney St., Suite 2800
Houston, Texas 77010
713-228-8600
713-228-8778 (fax)
Attorney for Applicants

379388_1